UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/792,062	03/02/2004	Jun Wang	030157	4204

23696 7590 08/04/2010

QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
DESIR, PIERRE LOUIS	

ART UNIT	PAPER NUMBER
2617	

NOTIFICATION DATE	DELIVERY MODE
08/04/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/792,062	WANG ET AL.	
	Examiner	Art Unit	
	PIERRE-LOUIS DESIR	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7-17,29,30 and 44-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,7-17,29,30 and 44-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to the independent claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 30 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 30 has been amended to include "a computer program product residing on a processor-readable medium and comprising processor-readable instructions…"

In particular, regarding "Subject Matter Eligibility of processor-readable medium," The Official Gazette (O.G.) of January 26, 2010, states:

> The United States Patent and Trademark Office (USPTO) is obliged to give claims their broadest reasonable interpretation consistent with the specification during proceedings before the USPTO. See In re Zletz, 893 F.2d 319 (Fed. Cir. 1989) (during patent examination the pending claims must be interpreted as broadly as their terms reasonably allow). **The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent. See MPEP 2111.01. When the broadest reasonable interpretation of a claim covers a signal per se, the claim must be rejected under 35 U.S.C. § 101 as covering non-statutory subject matter** (emphasis added). See In re Nuijten, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter) and Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101, Aug. 24, 2009; p. 2.

The USPTO recognizes that applicants may have claims directed to computer readable media that cover signals per se, which the USPTO must reject under 35 U.S.C. § 101 as covering

both non-statutory subject matter and statutory subject matter. In an effort to assist the patent community in overcoming a rejection or potential rejection under 35 U.S.C. § 101 in this situation, the USPTO suggests the following approach.

A claim drawn to such a computer readable medium that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "non-transitory" to the claim.

Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes signals per se. The limited situations in which such an amendment could raise issues of new matter occur, for example, when the specification does not support a non-transitory embodiment because a signal per se is the only viable embodiment such that the amended claim is impermissibly broadened beyond the supporting disclosure. See, e.g., Gentry Gallery, Inc. v. Berkline Corp., 134 F.3d 1473 (Fed. Cir. 1998).

Claim Objections

4. Claim 5 is objected to because of the following informalities: "location disclosure" should be "location distribution." Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 4-5, 7-17, 29-30, 44-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rice et al. (Rice, US 20030023726 A1) in view of Vanttinnen et al. (US 20010055394 A1).

Regarding claim 1, Rice disclose a method of providing location services (LCS) comprising receiving a request for location information for a mobile station from a location client (i.e., a client application submits a request to the system requesting location information for an identified information for a particular wireless communication device) (see paragraph 13); determining whether suitable location information is available from a cache (i.e., in response to the location request, the location server may retrieve location information from memory or alternatively, one or more of the LFEs may be prompted to obtain location information. In this regard, the location request may include a specification regarding the desired location information, for example, how recent or how accurate the information should be. If the memory includes information conforming to the specification, then this information is retrieved and output to a requesting application. Otherwise, appropriate information may be obtained by prompting one or more LFEs to locate the wireless communications device of interest (see paragraph 25). Thus, the location server would determine whether location information conforming to the specification included in the request for location information is available from the memory or cache); performing authorization for location distribution based on a first security procedure to determine whether the location client is authorized to receive the location information for the mobile station via a first network entity and performing authentication for the

location distribution based on the first security procedure to authenticate the location client (i.e., when a request for location information is made by a client application, before steps are performed in providing location information, the authentication and authorization process for most requests is performed) (see paragraph 14. Also refer to paragraphs 59-60 and 65); performing location determination to obtain location information for the mobile station responsive to the request for the location information when the suitable location information for the mobile station is unavailable (i.e., as described above, if location information from the cache does not conform to the specification included in the request for location information, the location server would prompt one or more LFEs to locate the wireless communications device of interest) (see paragraph 25); and performing location distribution via the first and second network entities to provide the location information for the mobile station responsive to the request for the location information (i.e., location information may be received from both the cache and the LFEs) (see paragraph 25), and skipping the location determination when the present location information for the mobile station is available from the cache (i.e., it is clear form the description in paragraph 25 that if the location information from the cache does conform to the specification that is included in the request, the location information is retrieved from the cache, and the LFEs would not be prompted for location determination, i.e., the location determination would be skipped (see paragraph 25).

Rice does disclose that the LFE may employ different location finding technologies, e.g., GPS, AOA, TDOA, and cell sector technologies to obtain the location of a subscriber's wireless device. One skilled in the art would have found it obvious that the LFE has to be authorized and

authenticated to be able to determine the location of the device. However, Rice does not describe such disclosure.

Thus, Rice does not specifically disclose performing authorization for location determination based on a second security procedure, independent of the first security procedure, to determine whether a second network entity is authorized for the location information for the mobile station; performing authentication for the location determination based on the second security procedure to authenticate the second network entity.

It should be noted that while the first authorization and authentication procedure was performed between the client application and the location server, the second authentication and authorization is performed between the location server and the "target" mobile device.

Vanttinnen discloses a mobile device comprising an integrated IP device. Both the mobile device and the integrated device are capable of determining its own location information. Vanttinnen discloses of a security association, which points from the IP device to the location server. The first security association allows the IP device to authenticate the location server and the second security association is used when the IP device determines its own location and it allows the IP device to transmit location information to the location server. The IP device may authorize the mobile station, which is capable of determining its own location, to grant a permission to transmit location information to the location server. After an authorization, the mobile station may transmit location information to the location server (see paragraphs 61 and 64).

Thus, one skilled in the art would find it to be obvious from the combination to have a client application requesting location information of a target mobile device from a location

server, which would prompt Location Finding Equipment (e.g., GPS) to determine the location of the target device (See Rice's paragraph 25). The location server would first authenticate and authorize the client application (as disclosed by Rice). If the location information stored in the cache does not conform to the specification required from the location request, the location server would prompt one or more LFEs to determine the location of the target device (see Rice's paragraph 25). Before location information may be sent to the location server, the mobile device or IP device which includes a built-in GPS receiver would authorize and authenticate the location server.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the proper protection in all aspects involved in the obtaining and transmitting of location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

Regarding claim 4, Rice discloses a method (see claim 1 rejection) as described above.

Rice does not specifically disclose a method further comprising performing a first session key setup to obtain a first session key, wherein the first session key is used for authentication and encryption of messages exchanged with the first network entity; and performing a second session key setup to obtain a second key, wherein the second session key is used for authentication and encryption of messages exchanged with the second network entity.

However, Vanttinnen discloses of a LCS client requesting location information has to be authenticated. There has to be a pre-negotiated contract between the cellular network operator

and the party requesting location information. When the contract is made, usually some secret authentication information is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key (i.e., first session key set up and key is used for authentication and encryption of messages exchanged) (see paragraph 9). Furthermore, Vanttinnen discloses that a second security association, which points from the IP device to authenticate the location server, and specifies encryption data. The location server and the IP device may establish security associations between themselves if they have a common key management center (i.e., performing second session key setup to obtain a second key which is used for authentication and encryption of messages exchanged between the location server and the IP device) (see paragraphs 61-63).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the proper protection in all aspects involved in the obtaining and transmitting of location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

Regarding claim 5, Rice discloses a method (see claim 1 rejection) wherein the location determination and the location disclosure are performed in two separate LCS sessions---
It should be noted that claim 1 has been amended by deleting the language related to "location disclosure" by adding language related to "location distribution." There is no longer support in claim 1 for the language related to “location disclosure.” And, in case examiner was to interpret

"location disclosure" and "location distribution", Rice discloses that location determination is done by prompting one or more LFEs to determine the location of the target device and "location disclosure" is performed by retrieving the location information from a cache or memory (see paragraph 25). Therefore, two separate sessions are used to perform "location distribution" and "location determination."

Regarding claim 7, the combination of Rice and Vanttinnen discloses a method (see claim 1 rejection) wherein the second network entity is located in a serving network for the mobile station (i.e., considering the second network entity is one of the LFE, as disclosed by Rice, the LFE, which includes a built-in GPS receiver is obviously located in the serving network of the mobile station (see Rice's paragraph 24 and Vanttinnen's paragraphs 8 and 64)) and the first network entity is located in a home network for the mobile station (i.e., the location server of Rice (see paragraphs 24-25) or the GMLC (which is communication with the location server) of Vanttinnen (see fig. 3).

Regarding claim 8, Rice discloses a method (see claim 1 rejection) wherein the location distribution is performed by a location client and a location server (i.e., the location server obtains the location information from a cache and transmits it to the location client, i.e., client application) (see paragraphs 24-25).

Regarding claim 9, Rice discloses a method (see claim 8 rejection) wherein the first network entity includes an LCS provider (i.e., client application or business provider) (see paragraph 51), and wherein the location client is located in the LCS provider (see paragraph 51).

Regarding claim 10, Rice discloses a method (see claim 8 rejection) wherein the first network entity includes an LCS server, and wherein the location server is located in the LCS

server (i.e., one skilled in the art would find it obvious that the location server is a LCS server or mobile station location server) (see fig. 1, item 50).

Regarding claim 11, Rice discloses a method (see claim 1 rejection) wherein second network entity includes a position determining entity (PDE) (i.e., LFEs) (see paragraphs 24-25).

Regarding claim 12, Rice discloses a method as described above (see claim 11 rejection).

Although Rice discloses a method as described, Rice does not specifically disclose a method wherein the second network entity further includes a serving mobile positioning center.

However, Vanttinnen discloses a method comprising a serving mobile location center (SMLC). Therefore, it would have been obvious to one of ordinary skill in the art to have combined the teachings of Vanttinnen with the teachings described by Rice to arrive at the claimed limitation in order to properly handle the location of mobile stations in the network the mobile station is currently in, which would ensure the accuracy of the location information.

Regarding claims 13 and 15, Rice discloses a method as described (see claim 1 rejection).

Although Rice discloses a method as described, Rice does not specifically disclose a method wherein the first network entity and the second network entity further includes a home authentication, authorization, and accounting entity.

However, Vanttinnen discloses a method wherein a GMLC interacts with both a first network entity (i.e., location server) (see fig. 3) and a second network entity (see paragraph 61), wherein the GMLC provides authentication and authorization for location services (see paragraphs 8 and 63). Also, it is well known in the art that GSM location service standards specify that GMLC must administer AAA policy towards any LCS client that requests location information. Thus one skilled in the art would find it obvious that both the first and second

network entity includes an H-AAA since they are both connected to the GMLC, which administer AAA policies.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the requesting client application or LCS client is entitled to receive the location information.

Regarding claim 14, Rice discloses a method (see claim 1 rejection) wherein the first network entity includes an LCS server (i.e., location server) (see fig. 1, paragraphs 24-25).

Regarding claim 16, Rice discloses a method (see claim 1 rejection) wherein the location information for the mobile station comprises a location estimate for the mobile station (i.e., Rice discloses in paragraph 24 that the location information include location uncertainty. Thus, thus one skilled in the art would have found it to be obvious that the location information is an estimate of the location information of the device).

Regarding claim 17, Rice discloses a method (see claim 1 rejection) wherein the location information for the mobile station further comprises an uncertainty for the location estimate for the mobile station (i.e., uncertainty information) (see paragraph 24).

Regarding claim 29, Rice discloses an apparatus comprising means for receiving a request for location information for a mobile station from a location client (i.e., a client application submits a request to the system requesting location information for an identified information for a particular wireless communication device) (see paragraph 13); means for performing location determination to obtain location information for the mobile station

responsive to the request for the location information when present location information for the mobile station is unavailable from a cache (i.e., in response to the location request, the location server may retrieve location information from memory or alternatively, one or more of the LFEs may be prompted to obtain location information. In this regard, the location request may include a specification regarding the desired location information, for example, how recent or how accurate the information should be. If the memory includes information conforming to the specification, then this information is retrieved and output to a requesting application. Otherwise, appropriate information may be obtained by prompting one or more LFEs to locate the wireless communications device of interest (see paragraph 25). Thus, the location server would determine whether location information conforming to the specification included in the request for location information is available from the memory or cache); means for performing location distribution via a second LCS session, independent of the first LCS session, to provide the location information for the mobile station to the location client responsive to the request for the location information, and skipping the location determination when the present location information for the mobile station is available from the cache (i.e., location information may be received from both the cache and the LFEs. It is clear form the description in paragraph 25 that if the location information from the cache does conform to the specification that is included in the request, the location information is retrieved from the cache, and the LFEs would not be prompted for location determination, i.e., the location determination would be skipped) (see paragraph 25).

Rice does not specifically disclose an apparatus comprising means performing a first session key setup to obtain a first session key, wherein the first session key is used for authentication and encryption of messages exchanged between a first network entity and the

mobile station; and means for performing a second session key setup to obtain a second key, wherein the second session key is used for authentication and encryption of messages exchanged between a second network entity and the location client.

However, Vanttinnen discloses of a LCS client requesting location information has to be authenticated. There has to be a pre-negotiated contract between the cellular network operator and the party requesting location information. When the contract is made, usually some secret authentication information is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key (i.e., second session key set up and key is used for authentication and encryption of messages exchanged between the location client application and GMLC/location server) (see paragraph 9). Furthermore, Vanttinnen discloses that a second security association, which points from the IP device to authenticate the location server, and specifies encryption data. The location server and the IP device may establish security associations between themselves if they have a common key management center (i.e., performing first session key setup to obtain a first key which is used for authentication and encryption of messages exchanged between the location server and the IP device) (see paragraphs 61-63).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the proper protection in all aspects involved in the obtaining and transmitting of

location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

Regarding claim 30, Rice discloses a computer program product residing on a non-transitory processor-readable medium and comprising processor-readable instructions configured to cause the processor to authenticate, based on a first session obtained using a first security procedure, a location client requesting location information of a mobile station via a home network and obtain location information for the mobile station responsive to the authenticated request for location information for the mobile station when present location information for the mobile station is unavailable from a cache (i.e., a client application submits a request to the system requesting location information for an identified information for a particular wireless communication device (see paragraph 13). In response to the location request, the location server may retrieve location information from memory or alternatively, one or more of the LFEs may be prompted to obtain location information. In this regard, the location request may include a specification regarding the desired location information, for example, how recent or how accurate the information should be. If the memory includes information conforming to the specification, then this information is retrieved and output to a requesting application. Otherwise, appropriate information may be obtained by prompting one or more LFEs to locate the wireless communications device of interest (see paragraph 25). Thus, the location server would determine whether location information conforming to the specification included in the request for location information is available from the memory or cache). Furthermore, Rice discloses that when a request for location information is made by a client application, before steps are performed in providing location information, the

authentication and authorization process for most requests is performed) (see paragraph 14. Also refer to paragraphs 59-60 and 65); and provide. From a serving network, the location information to the location client responsive to the request for the location information for the mobile station and skip obtaining the location information when present location information for the mobile station is available from the cache (i.e., location information may be received from both the cache and the LFEs. It is clear form the description in paragraph 25 that if the location information from the cache does conform to the specification that is included in the request, the location information is retrieved from the cache, and the LFEs would not be prompted for location determination, i.e., the location determination would be skipped) (see paragraph 25).

Rice does disclose that the LFE may employ different location finding technologies, e.g., GPS, AOA, TDOA, and cell sector technologies to obtain the location of a subscriber's wireless device. One skilled in the art would have found it obvious that the LFE has to be authorized and authenticated to be able to determine the location of the device. However, Rice does not describe such disclosure.

Thus, Rice does not specifically disclose authenticate the mobile station for location determination responsive to the request for location information based on a second security procedure, independent of the first security procedure.

It should be noted that while the first authorization and authentication procedure was performed between the client application and the location server, the second authentication and authorization is performed between the location server and the "target" mobile device.

Vanttinnen discloses an integrated IP device. Both the mobile device and the integrated device are capable of determining its own location information. Vanttinnen discloses of a security association, which points from the IP device to the location server. The first security association allows the IP device to authenticate the location server and the second security association is used when the IP device determines its own location and it allows the IP device to transmit location information to the location server. The IP device may authorize the mobile station, which is capable of determining its own location, to grant a permission to transmit location information to the location server. After an authorization, the mobile station may transmit location information to the location server (see paragraphs 61 and 64).

Thus, one skilled in the art would find it to be obvious from the combination to have a client application requesting location information of a target mobile device from a location server, which would prompt Location Finding Equipment (e.g., GPS) to determine the location of the target device (See Rice's paragraph 25). The location server would first authenticate and authorize the client application (as disclosed by Rice). If the location information stored in the cache does not conform to the specification required from the location request, the location server would prompt one or more LFEs to determine the location of the target device (see Rice's paragraph 25). Before location information may be sent to the location server, the mobile device or IP device which includes a built-in GPS receiver would authorize and authenticate the location server.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been

to ensure the proper protection in all aspects involved in the obtaining and transmitting of location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

Regarding claim 44, Rice discloses a method of providing location services comprising receiving a request, from a location client, for location disclosure of a mobile station (i.e., a client application submits a request to the system requesting location information for an identified information for a particular wireless communication device) (see paragraph 13); authenticating the request using a secure disclosure session between a network entity and the location client (i.e., when a request for location information is made by a client application, before steps are performed in providing location information, the authentication and authorization process for most requests is performed) (see paragraph 14. Also refer to paragraphs 59-60 and 65); determining whether cached location information is available and if the cached location information is available, responding to the request for location disclosure with the location information in the secure disclosure session, and if the cached location information is not available, initiating a request for location determination (i.e., in response to the location request, the location server may retrieve location information from memory or alternatively, one or more of the LFEs may be prompted to obtain location information. In this regard, the location request may include a specification regarding the desired location information, for example, how recent or how accurate the information should be. If the memory includes information conforming to the specification, then this information is retrieved and output to a requesting application. Otherwise, appropriate information may be obtained by prompting one or more LFEs to locate the wireless communications device of interest (see paragraph 25). Thus, the

location server would determine whether location information conforming to the specification included in the request for location information is available from the memory or cache. When a request for location information is made by a client application, before steps are performed in providing location information, the authentication and authorization process for most requests is performed (see paragraph 14. Also refer to paragraphs 59-60 and 65). As described above, if location information from the cache does not conform to the specification included in the request for location information, the location server would prompt (i.e., **initiate a request for location determination**) one or more LFEs to locate the wireless communications device of interest) (see paragraph 25).

Rice, however, does not specifically disclose a method wherein the authenticating steps involves authenticating the request using a secure disclosure session key, and the method comprises establishing a secure determination session between the network and the mobile station, independent of the secure disclosure session, to authenticate the request for location determination; and communicating location information within the secure determination session

Vanttinnen discloses a mobile device comprising an integrated IP device. Both the mobile device and the integrated device are capable of determining its own location information. Vanttinnen discloses of a security association, which points from the IP device to the location server. The first security association allows the IP device to authenticate the location server and the second security association is used when the IP device determines its own location and it allows the IP device to transmit location information to the location server. The IP device may authorize the mobile station, which is capable of determining its own location, to grant a permission to transmit location information to the location server. After an authorization, the

mobile station may transmit location information to the location server (see paragraphs 61 and 64).

Vanttinnen also discloses of a LCS client requesting location information has to be authenticated. There has to be a pre-negotiated contract between the cellular network operator and the party requesting location information. When the contract is made, usually some secret authentication information is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key (i.e., first session key set up and key is used for authentication and encryption of messages exchanged) (see paragraph 9)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the proper protection in all aspects involved in the obtaining and transmitting of location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

Regarding claim 45, Rice discloses a method as described (see claim 44 rejection).

Although Rice discloses a method as described, Rice does not specifically disclose a method wherein the request comprises receiving a request for the secure disclosure session key; and providing the secure disclosure session key in response to successful authentication and validation of the request for the secure session key.

However, Vanttinnen discloses of a LCS client requesting location information has to be authenticated. There has to be a pre-negotiated contract between the cellular network operator

and the party requesting location information. When the contract is made, usually some secret authentication information is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key (i.e., first session key set up and key is used for authentication and encryption of messages exchanged) (see paragraph 9). Furthermore, Vanttinnen discloses that a second security association, which points from the IP device to authenticate the location server, and specifies encryption data. The location server and the IP device may establish security associations between themselves if they have a common key management center (i.e., performing second session key setup to obtain a second key which is used for authentication and encryption of messages exchanged between the location server and the IP device) (see paragraphs 61-63).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the proper protection in all aspects involved in the obtaining and transmitting of location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

Regarding claims 46 and 47, Rice discloses a method as described (see claim 44 rejection).

Although Rice discloses a method as described, Rice does not specifically disclose a method wherein authenticating the request comprises mutually authenticating the location client and a first network entity of the network, and wherein establishing the secure determination

session comprises mutually authenticating the mobile station and a second network entity of the network, and wherein the first and second network entities are a single network entity.

However, However, Vanttinnen discloses of a LCS client requesting location information has to be authenticated. There has to be a pre-negotiated contract between the cellular network operator and the party requesting location information. When the contract is made, usually some secret authentication information is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key (i.e., first session key set up and key is used for authentication and encryption of messages exchanged) (see paragraph 9). Furthermore, Vanttinnen discloses that a second security association, which points from the IP device to authenticate the location server, and specifies encryption data. The location server and the IP device may establish security associations between themselves if they have a common key management center (i.e., performing second session key setup to obtain a second key which is used for authentication and encryption of messages exchanged between the location server and the IP device) (see paragraphs 61-63). Vanttinnen also disclose a method wherein the first and second network entities are a single network entity (i.e. GMLC) (see paragraphs 8, 61 and 63).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Vanttinnen with the teachings described by Rice to arrive at the claimed invention. A motivation for doing so would have been to ensure the proper protection in all aspects involved in the obtaining and transmitting of location information of a target device, which would eliminate the danger of attempts by unauthorized entities or individuals.

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rice and Vanttinnen, further in view of view of Horn.

Regarding claim 3, the combination discloses a method as described in claim 1 reasoning.

Although the combination discloses a method as recited above, the combination does not specifically disclose a method, wherein the first security procedure is based on an MD-5 algorithm and the second security procedure is based on an Authentication and Key Agreement (AKA) procedure.

However, Horn discloses security measures based on both MD-5 algorithm and Authentication and Key Agreement (AKA) (see col. 3, lines 44-50; col. 5, lines 20-41).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Horn with the teachings described by Rice and Vanttinnen to arrive at the claimed invention. A motivation to do so would have been to insure the security of the location determination/disclosure procedure.

8. Claims 48-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanttinnen in view of Rice.

Regarding claim 48, Vanttinnen discloses a system in a wireless communication network, the system comprising: a home network server (i.e. GMLC) configured to receive a request from a location client for location disclosure of a mobile station (i.e., a GMLC receives a location request from a location client) (see paragraph 8); authenticate the request using a secure disclosure session key and a secure disclosure session with the location client (i.e., the GMLC

authenticates the LCS client to make sure that it is entitled to receive location information (see paragraph 8). The party requesting location information is usually authenticated, because location information generally needs to be treated in a confidential manner. Generally, there has to be a pre-negotiated contract between the cellular network operator and the party requesting location information. When the contract is made, usually some secret authentication information (for example a shared key) is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key. The GMLC has its copy of the secret keys relating to the LCS Clients, for example. When an LCS Client, for example, tells it identity, the GMLC can then check using its copy of the a secret key that the LCS Client encrypted the text with the correct key) (see paragraph 9); and a serving network server (i.e., GMLC) communicatively coupled to the home network server (as can be seen from claim 50 description, both the home server and the serving server may be a single server) and configured to: establish a secure determination session, independent of the secure disclosure session, to authenticate the mobile station determine the location information of the mobile station and communicate the location information to the home network server (i.e., Vanttinnen discloses a mobile device comprising an integrated IP device. Both the mobile device and the integrated device are capable of determining its own location information. Vanttinnen discloses of a security association, which points from the IP device to the location server. The first security association allows the IP device to authenticate the location server and the second security association is used when the IP device determines its own location and it allows the IP device to transmit location information to the location server. The IP device may authorize the mobile station, which is capable of

determining its own location, to grant a permission to transmit location information to the location server. After an authorization, the mobile station may transmit location information to the location server) (see paragraphs 61 and 64).

Vanttinnen does not specifically disclose a system comprising determine whether cached location information is available; respond to the request for location disclosure with the location information in the secure disclosure session if the cached location information is available; and initiate a request for location determination if the cached location information is not available.

However, Rice discloses a system wherein in response to the location request, a location server may retrieve location information from memory or alternatively, one or more of the LFEs may be prompted to obtain location information. In this regard, the location request may include a specification regarding the desired location information, for example, how recent or how accurate the information should be. If the memory includes information conforming to the specification, then this information is retrieved and output to a requesting application. Otherwise, appropriate information may be obtained by prompting one or more LFEs to locate the wireless communications device of interest (see paragraph 25). Thus, the server would determine whether location information conforming to the specification included in the request for location information is available from the memory or cache. Also, Rice discloses that when a request for location information is made by a client application, before steps are performed in providing location information, the authentication and authorization process for most requests is performed) (see paragraph 14. Also refer to paragraphs 59-60 and 65).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings as described by Rice with the teachings described by

Vanttinnen to arrive at the claimed invention. A motivation for doing so would have been to provide up-to-date and accurate location information to the requesting entity, and location information that conforms to the specification indicated in the received location information request.

Regarding claim 49, Vanttinnen discloses a home network server (see claim 48 rejection) that is configured to perform mutual authentication with the location client and to provide the location information to the location client, and wherein the serving network server is configured to perform mutual authentication with the mobile station (i.e., There has to be a pre-negotiated contract between the cellular network operator and the party requesting location information. When the contract is made, usually some secret authentication information is exchanged, and for each request, the party has to present it possesses this secret authentication information, for example by encrypting a part of the location request message with the secret key (i.e., first session key set up and key is used for authentication and encryption of messages exchanged) (see paragraph 9). Furthermore, Vanttinnen discloses that a second security association, which points from the IP device to authenticate the location server, and specifies encryption data. The location server and the IP device may establish security associations between themselves if they have a common key management center (i.e., performing second session key setup to obtain a second key which is used for authentication and encryption of messages exchanged between the location server and the IP device) (see paragraphs 61-63). Vanttinnen also disclose a method wherein the first and second network entities are a single network entity (i.e. GMLC)) (see paragraphs 8, 61 and 63).

Regarding claim 50, Vanttinnen discloses a system (see claim 50 rejection) wherein the home and serving network servers are a single server (i.e., GMLC) (see paragraphs 8, 61-63)

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PIERRE-LOUIS DESIR whose telephone number is (571)272-7799. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dwayne Bost can be reached on (571)272-7023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PIERRE-LOUIS DESIR/
Examiner, Art Unit 2617